CLAIMS

1. A packets sending/receiving apparatus for sending a sending packets and receiving a receiving packets, comprising:

authentification and key exchange means for producing an encryption key and a decoding key;

encryption means for producing an encryption sending data by encrypting sending data using the encryption key;

sending condition setting management means for producing sending condition setting information for setting sending condition of the sending packets using at least one of sending condition related information, sending /reception management information, receiving condition setting information;

packetization means for producing the sending packets using the encryption sending data;

receiving condition setting management means for producing receiving condition setting information for setting receiving condition of the receiving packets using at least one of receiving condition related information and packets reception information;

packets reception means for receiving the reception packets, which extracts reception data included in the reception packets from the reception packets using the reception condition setting information and produced the packets reception information from the reception packets, and outputs the packets reception information to the authentification and key exchange means or the received condition setting management means; and

decoding means for decoding the reception data using the decoding key.

2. A packets sending/receiving apparatus according to claim 1, wherein:

the packetization means includes a packets addition information production means for producing packets addition information using at least one of the sending condition

setting information and authentification and key exchange related information related to the authentification and key exchange means,

the packetization means produces the sending packets by adding packets addition information to the encryption sending data; and

the packets receiving means includes a packets addition information extraction means for extracting the packets addition information included in the sending packets.

3. A packets sending/receiving apparatus according to claim 1, further comprising:

framing means for receiving the sending packets to produce a sending frame; and

frame reception means for receiving a reception frame and extracting the reception packets from the reception frame.

4. A packets sending/receiving apparatus according to claim 1, further comprising:

first queue means for temporarily stores first packets produced at the packetization means;

second queue means for temporarily stores second packets produced at the packetization means;

sending queue control means for controlling which of the first packets stored in the first queue means and a second packets stored in the second queue means is to be sent based on the sending condition setting information;

framing means for producing a sending frame by framing the first packets output from the first queue means and the second packets output from the second queue means; and

a frame reception means for extracting the reception packets from a reception frame.

5. A packets sending /receiving apparatus according to claim 4, wherein the sending queue control means controls which of the first packets group stored in the first queue means and a second packets group stored in the second queue means is to be sent

using at least one of information regarding a sending path of the first packets group or the second packets group, information regarding a bandwidth required for sending the first packets group or the second packets group, information regarding delay from sending to arrival of the sending packets, and information regarding priority of the first packets or the second packets.

6. A packets sending/receiving apparatus according to claim 5, wherein the sending queue control means uses one of control schemes of RSVP scheme described with IETF RFC2205, RFC2208, RFC2209,Intserv scheme described with IETF RFC2210, RFC2211, 2212, RFC2215, and Diffserv scheme described with IETF RFC2474, RFC2475, RFC2597, RFC2598.

7. A packets sending/receiving apparatus according to claim 4, wherein the sending queue control means controls the first queue means and the second queue means so as to select one of the first packets group stored in the first queue means and the second packets group stored in the second queue means is to be sent and preferentially outputs the selected packets.

8. A packets sending/receiving apparatus according to claim 4, the sending queue control means controls the first queue means and the second queue means such that, when an amount the first packets group stored in the second queue means does riot exceeds a predetermined amount, the first packets group stored in the first queue means is preferentially output, and when an amount of the second packets group stored in the second queue means exceeds a predetermined amount, the second packets group stored in the second queue means is output preferentially.

9. A packets a ending/ receiving apparatus according to claim 4, wherein the sending queue control means controls the first queue means and the second queue means so as to average intervals between the first packets group sent from the first queue means and the second packets group from the second queue means.

10. A packets sending/receiving apparatus according to claim 1, wherein the receiving condition setting management means and the receiving condition setting

management means detect the maximum transmission packet size in a path from a sending destination of the sending packets and a receiving address between sending and arrival of the sending frame, and produces the sending condition setting information and receiving condition setting information using the maximum transmission packet size information.

11. A packets sending/receiving apparatus according to claim 3, wherein the framing means adds a frame header of IEE 802.3 standard to sending packets produced in the packetization frame.

12. A packets sending/receiving apparatus according to claim 3, wherein the framing means adds a frame header of IEE 802.1Q standard to sending packets produced in the packetization frame.

13. A packets sending/receiving apparatus according to claim 1, wherein the packetization means converts the encryption sending data to a predetermined size and adds Internet Protocol (IP) header defined as IPv4 or IPv6 in IETF.

14. A packets sending/receiving apparatus according to claim 1, wherein the packetization means adds information indicating that it is a preferred packet to a service type field of IPv4 header or a type of service (TOS) field in the service type field.

15. A packets as apparatus according to claim 1, wherein the packetization means adds information indicating that it is a preferred packet to a priority field of IPv6 header.

16. A packets sending/receiving apparatus according to claim 4, wherein:

the packetization means includes first packetizatton means and second packetization means;

the first packetization means produces a first packets group using at least one of the sending condition setting information, and the authentification and key exchange related information;

the second packetization means produces a second packets group using at least one of the sending condition setting information, authentification and key exchange related information, and the encryption sending data.

17. A packets sending/receiving apparatus according to claim 16, wherein:

the packetization means converts the encryption sending data into a predetermined size and adds an IP header defined as IPv4 or IPV6 in IETF;

the first packetization means is formed of a software, and the second packetization means is formed of a hardware.

18. A packets sending/receiving apparatus according to claim 16, further comprising:

data separation means for separating the reception data into preferred data and general data;

the encryption means encrypts the preferred data; and

the first packetization means produces a first packets group using the general data.

19. A packets sending/receiving apparatus according to claim 18, wherein the first packetization means adds at least one header of RTCP, RTSP, HTTP, TCP, UDP, IP, which are data process protocols defined in the IETF document.

20. A packets sending/receiving apparatus according to claim 18, wherein the second packetization means adds a sequence number to data, or adds at least one header of RTP, UDP, HTTP, TCP, IP, which are data process protocols defined in the IETF document.

21. A packets sending/receiving apparatus according to claim 18, wherein the preferred data is in an uncompressed SD format signal defined by SMPTE 259M standard, an uncompressed HD format defined by SMPTE 292 standard, a transmission stream format of DV or MPEG-TS by IEEE 1394 defined by IEC 61883, MPEG-TS format by DVB-ASI defined by DVB standard A010, MPEG-PS format, MPEG-ES format, and MPEG-PES format.

22. A packets sending/receiving apparatus according to claim 16, wherein the second packetization means includes error correction code addition means.

23. A packets sending/receiving apparatus according to claim 22, wherein a scheme of the error correction code used in the error correction code addition means is Reed-Solomon scheme or parity scheme.

24. A packets sending/receiving apparatus according to claim 16, wherein information indicating the encryption key outputs decoding information of the encryption key before the encrypted sending packets encrypted with the encryption key is output in the framing means.

25. A packets sending/receiving apparatus according to claim 24, wherein information indicating the encryption key sent before the time of reception of a reception frame which corresponds to the sending frame from sending of the sending frame with respect to the time when the receiving packets including the encryption sanding data produced using the encryption key is sent.

26. A packets sending/receiving apparatus according to claim 1, wherein the authentifieation and key change means permits authentification when location information of the packets sending/receiving apparatus, and location information of the destination of the sending packets or location information of the source of the receiving packets match predetermined condition.

27. A packets sending/receiving apparatus according to claim 26, wherein the sending/receiving management information includes at least one of the location information of the packets sending/receiving apparatus, and the location information of the destination of the sending packets or the location information of the source of the receiving packets match predetermined condition.

28. A packets sending/receiving apparatus according to claim 27, wherein the location information is information with area specified by a region code, address, postal code, or longitude and latitude.

29. A packets sending/receiving apparatus according to claim 26, wherein the authentification and key exchange means permits authentification when a propagation time of one-way or a round trip from the packets sending/receiving apparatus to the destination

of the sending packets or sending source of the reception packets is shorter than a predetermined limit time between the packets sending/receiving apparatus to the destination of the sending packets or sending source of the reception packets.

30. A packets sending/ receiving apparatus according to claim 1, wherein the authentification and key exchange means permits authentification, in the case where there is a wireless transmission zone between a sending/reception zone between the packets sending/ receiving apparatus to the destination of the sending packets or sending source of the reception packets, when it is confirmed that it is in a mode for scrambling and transmitting data in the wireless transfer zone.

31. A packets sending/receiving apparatus according to claim 26, wherein the authentification and key exchange means includes:

storage means for temporarily stores information regarding the destination of the sending packets or sending source of the reception packets when authentification is performed between the packets sending/receiving apparatus to the destination of the sending packets or sending source of the reception packets;

verifying means for verifying the information stored in the storage means and the information regarding the destination of the sending packets or the information regarding the sending source of the reception packets when authentification is not confirmed since the packets sending/receiving apparatus and the destination of the sending packets or sending source of the reception packets do not match the predetermined conditions, and performing authentification between the packets sending/receiving apparatus and the destination of the sending packets or sending source of the reception packets.

32. A packets sending/receiving apparatus according to claim 31, the information regarding the destination of the sending packets and the information regarding the sending address of the reception packets includes at least one of a certificate, MAC address and biometric information.

33. A packets sending/receiving apparatus according to claim 1, wherein the authentification and key exchange means performs predefined authentification and key exchange and updates encryption key or decoding key in a predetermined period.

34. A packets sending/receiving apparatus according to claim 33, wherein timing information for indicating timing for the authentification and key exchange means to update the decoding key is added to the sending packets.

35. A packets sending/receiving apparatus according to claim 33, wherein the timing for the authentification and key exchange means to update the decoding key is notified by changing a TCP port number, or UDP port number of the sending packets.

36. A packets sending/receiving apparatus according to claim 33, wherein the timing for the authentification and key exchange means to update the decoding key is updated for every HTTP request when the sending packets use HTTP.

37. A packets sending/receiving apparatus according to claim 33, wherein the timing for the authentification and key exchange means to update the decoding key is changed for every certain amount of data when the sending packets use HTTP.

38. A packets sending/receiving apparatus according to claim 33, wherein the receiving source of the reception packets is updated within a predetermined period when the sending packets use RTP.

39. A packets sending/receiving apparatus according to claim 33, wherein copy control information of DTCP scheme in the authentification and key exchange means is transmitted by adding encryption mode information to the reception packets.

40. A packets sending/receiving apparatus according to claim 19, wherein the sending queue control means controls the first queue means and the second queue means such that data rate of the preferred data does not become smaller than a predetermined value.

41. A packets sending/receiving apparatus according to claim 40, wherein the sending queue control means controls the first queue means and the second queue means

such that the time for the preferred data to be stored in the second queue means is always smaller than a predetermined value.

42. A packets sending/receiving apparatus according to claim 40, wherein:

the second packetization means includes a buffer means for temporarily storing data, a counter means for counting a length of the data, a packets header production means for producing packets header of the second packets group, and a packets synchronization means for synchronizing packets by combining packet headers and payload output from the buffer; and

the packets header production means specifies a payload length of the second packets, reads out the data stored in the buffer means, and input to the packets synchronization means.

43. A packets sending /receiving apparatus according to claim 40, wherein:

the second packetization means includes a buffer means for temporarily storing data extracted from the preferred data, a counter means for counting a length of the data, a packet header production means for producing a packet header using packetization information, and a packet production means for producing packets by combining the packet headers and payload; and

the counter means outputs control data for reading out data which corresponds to a payload length from the buffer means.

44. A packets sending/receiving apparatus according to claim 40, wherein:

the second packetization means includes a buffer means for temporarily stores data, a counter means for counting the data, a packet header production means for producing a packet header using packetization information, error correction addition means for adding error correction to the data, and a packets synchronization means for synchronizing the packet header and the data with the error correction added; and

the counter means outputs control data for reading out data which corresponds to a payload length from the buffer means.

45. A packets sending/receiving apparatus according to claim 40, wherein, in a layer for processing a reception frame of a layer lower than layers on which the preferred data and the general data are processed, the preferred data and the general data rare selected from the communication protocol header of the reception packets included in the reception frame, and a process for the preferred data and a process for the general data are independently performed.

46. A packets sending/receiving apparatus according to claim 1, the second packetization means includes encryption switching means, and input an encryption key input to the encryption key switching means while switching the encryption key in the encryption means at a specified timing.

47. A packets sending/receiving apparatus according to claim 46, wherein timing used for the encryption key switching is timing generated in synchronization with a predetermined sequence number in a packet header, which is an output for the packet header production means.

48. A packets sending/receiving apparatus according to claim 46, wherein the timing for the authentification and key exchange means to update the decoding key is updated for every HTTP request when the sending packets use HTTP.

49. A packets sending/receiving apparatus according to claim 46, wherein the timing for the authentification and key exchange means to update the decoding key is changed for every certain amount of data when the sending packets use HTTP.

50. A packets sending/receiving apparatus according to claim 46,.wherein timing for the authentification and key exchange means to update the decoding key is within a predetermined period when the sending packets use RTP.

51. A packets sending/receiving apparatus according to claim 46, wherein timing used for the encryption key switching is timing generated in synchronization with an endpoint and a start point of an error correction matrix.